ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE: ARTICLE: OUTRUN THE LIONS: A PRACTICAL FRAMEWORK FOR ANALYSIS OF LEGAL ISSUES IN THE EVOLUTION OF CLOUD COMPUTING

Winter, 2014

Reporter
12 Ave Maria L. Rev. 71 *

Length: 27747 words

Author: Kenneth N. Rashbaum+, Bennett B. Borden++ and Theresa H. Beaumont+++

+ Kenneth N. Rashbaum is Principal of Rashbaum Associates, L.L.C. in New York. His practice focuses on counsel to healthcare organizations and multinational corporations on privacy, data protection, and information governance across borders, regulatory compliance, and litigation. He is a frequent speaker and writer in the areas of cross-border discovery and disclosure conflicts, international information governance, and health information compliance and management. Mr. Rashbaum is Co-Chair of the International Litigation Committee of the American Bar Association Section of International Law and an Adjunct Professor of Law at the Maurice A. Deane School of Law at Hofstra University.

++ Bennett B. Borden is a partner at Drinker Biddle & Reath LLP and Chair of its Information Governance and E-Discovery Group. He is also an officer of the firm's e-discovery subsidiary, Drinker Discovery Solutions, L.L.C., which provides state of the art e-discovery technology and services to the firm's clients. Bennett is a globally recognized authority on the legal, technology, and policy implications of digital information. He is Chair of the Cloud Computing Committee and Vice Chair of the Electronic Discovery and Digital Evidence Committee of the Science and Technology Law Section of the ABA, and a founding member of the steering committee for the Electronic Discovery Section of the District of Columbia Bar.

+++ Theresa H. Beaumont, of Groupe Beaumont, Inc., advises clients on strategic use of technology for Information Governance challenges. Most recently, as Google's Global E-Discovery Counsel (2008-2012), Ms. Beaumont developed its discovery response team for litigation, competition and regulatory investigations. Ms. Beaumont also participated in product development for Cloud Information Governance and eDiscovery solutions. Prior to joining the company, Ms. Beaumont handled complex litigation management and technology issues within the internet startups and in private practice. Ms. Beaumont also co-chairs the American Bar Association's Interest and Cloud Computing Committee of the Science and Technology Law Section, is a member of the Sedona Conference, and serves on the Advisory Board of Georgetown University's Advanced E-Discovery Institute. Ms. Beaumont received her J.D. from Northwestern University School of Law and her undergraduate degree in Philosophy from Hope College.

Highlight

Every morning in Africa, a gazelle wakes up.

It knows it must run faster than the fastest lion or it will be killed.

Every morning a lion wakes up.

It knows it must outrun the slowest gazelle or it will starve to death.

It doesn't matter whether you are a lion or a gazelle.

When the sun comes up, you better start running. [1]

Text

[*72]

Introduction

There is something about Cloud Computing that is fundamentally different. But is there a significant difference in the laws that govern it, or do we merely need to look at already established legal principles that govern it in a more holistic way? True, cloud technology has changed the way we interact with each other. We communicate, socialize, work with, sell to, and buy from each other in ways unimaginable a generation ago, due in large measure to the advent of the Internet or, more colloquially, the Cloud. The impact of the Cloud cannot be overstated. For example, most social media are based in Cloud technology. Social media have changed the paradigm of interpersonal communication, to sharing thoughts and activities in ways previously impossible and, not so long ago, impolite; to their uses in organizing movements that have toppled governments, such as in Egypt and other countries during the "Arab Spring"; [2] to securing the assistance of the public for law enforcement to such an extent that the suspects of the Boston Marathon bombings in April 2013, were apprehended within days because the requests for videos and photos that could depict the identities of the suspects - many such images were, in fact, posted on social media - were sent to millions within minutes on social media sites, using Cloud technology. [3]

Indeed, law is fundamentally society's commentary on interaction; it rewards reasonable conduct and punishes unreasonable conduct. But, for the most part, a legislature or court does not comment on a particular type of interaction until it has already occurred and its consequences have played out. Many types of interactions that have sprung from the Information Age are new in degree and sometimes in kind, and so there is often little or no law to guide those interactions. For every advantage Cloud Computing offers - such as cost-efficiency, flexibility and scalability - there are risks associated with legal and regulatory compliance, data control, security, privacy, legal **[*73]** ethics, and determinations of reasonableness of the utilization of Cloud services. Contrary to the belief of many, it is well within our capabilities to analyze these legal quandaries and counsel clients appropriately in the Age of the Cloud - even without established case law or statutes - as long as we know, like the gazelle and the lion, that we have to run to succeed. And like the lion and the gazelle, we must rely on instincts to do so. For lawyers, this means applying established legal principles in new ways.

We live in an age of marvels, but we see them through frames of reference that were constructed over many years and, as a result, we typically do not quite run fast enough to keep up with the pace of technological advances. The digitization of information and the development of the infrastructure to largely decentralize and widely distribute it

---

[1] Thomas L. Friedman, The World is Flat: A Brief History of the Twenty-First Century 114 (1st ed. 2005).

[2] Everette E. Dennis et al., How People in the Middle East Actually Use Social Media, The Atlantic, Apr. 24, 2013, http://www.theatlantic.com/international/archive/2013/04/how-the-people-in-the-middle-east-actually-use-social- media/275246/; Agence France-Presse, Debate Flares Over Impact of Social Media on Arab Spring and Other "Revolutions', Raw Story, Mar. 10, 2013, http://www.rawstory.com/rs/2013/03/10/debate-flares-over-impact-of-social-media-on-arab-spring-and-other-revolutions/.

[3] Kevin F. Adler, Boston Bombings: Come Together, Right Now, on Social Media, The Christian Sci. Monitor, Apr. 26, 2013, http://www.csmonitor.com/Commentary/Opinion/2013/0426/ Boston-bombings-Come-together-right-now-on-social-media; Dan Gilgoff & Jane J. Lee, Social Media Shapes Boston Bombings Response, Nat'l Geographic Daily News, Apr. 15, 2013, http://news.nationalgeographic.com/news/2013/13/130415-boston-marathon-bombings-terrorism-social-media-twitter- facebook.

through the Cloud, have given rise to an age that has changed the way we interact with each other in new ways. Yet, the fact that there may be little or no law regarding some of these new interactions does not mean that there is no guidance on how to conduct oneself. Every time a new kind of technology fundamentally alters our interactions, society has to sort out how to deal with them, and develop laws governing them. Some examples include the advent of the telegraph replacing the pony express, the telephone replacing the telegraph, the rise of locomotives and automobiles, and the widespread use of electrification. Each of these technologies or applications of technology changed how we interacted and the law developed to reward the "right" kinds of interaction and punish the "wrong" kinds.

Accordingly, in order to provide effective counsel and thereby avoid being "eaten" like the gazelles in the African proverb above, in such times of change, lawyers better start running. Where do they start, and how? They can start their analysis at the beginning, of course. How did the laws governing new interactions develop, and how can counselors keep up by providing guidance to those entering the new frontier? Lawyers can, and should, fall back on key principles of the laws of human interaction. For example, when the telegraph was invented, a signal was sent across a wire, and thus could be intercepted along its way. This was a new kind of intrusion that the law had not specifically encountered before. But it did have experience with certain corollaries, such as the theft of a letter in transit in the post, or eavesdropping outside an open window. Thus, by applying the already developed norms for dealing with human interaction, and extrapolating them to the new forms, successful lawyers were able to provide cogent counsel to their clients.

This Article outlines a practical framework for analyzing legal issues potentially arising from ownership, use, and disclosure of data in the Cloud, **[*74]** leveraging existing principles to guide practitioners and the bench in this evolving technology. The framework approach was selected because of two factors: the nascent state of the case law and the evolving nature of Cloud technology. A framework for analysis, then, in which the steps to analyzing a particular legal issue are discussed, was deemed of greater utility than a set of principles, which may become outmoded quickly as the case law develops and technology evolves.

The authors suggest the following framework for analyzing cloud legal issues.

A Practical Framework for Analysis of Legal Issues in the Evolution of Cloud Computing

I. Understanding Cloud Data from an Information Governance Perspective: Considerations for Decisions to Send Data to the Cloud, Get It Back Again and Use It

A. The Character of Cloud Data

1. Cross-Border Concerns: Storage and Transfer of Cloud Data

2. U.S. Privacy Considerations

B. Physical Possession: Who Has Control and Access, and How is the Data Controlled/Accessed by the Cloud Customer and Cloud Service Provider (CSP)?

C. Subpoenas, Government Agency Demands and Civil Discovery Requests

1. Subpoenas Served on the Cloud Customer

2. Subpoenas Served on the CSP

D. How is Discovery of Cloud Data Obtained?

1. Can Cloud Data Be Preserved As Required By Law? Information Management, Identification and Preservation, and Legal Holds

2. Spoliation and Sanctions - Does Data in the Cloud Have an Impact?

3. How Is the Data Collected from the Cloud? Data Export: Application Programming Interfaces (APIs) and Other Cloud Tools

a. Searching Cloud Data

b. Collection and Production of Cloud Data

c. How Can Cloud Data Be Used As Evidence At Trial? Rule 26(b)(2)(B) and Admissibility Information Collected from the Cloud

4. Admissibility - Authentication and Other Foundation Issues for Cloud Data

[*75]

I. Understanding Cloud Data from an InformationGovernance Perspective

Information, especially electronic information, is a vital corporate asset. Its creation, use, maintenance, disclosure, and disposition is at the heart of Information Governance, and Information Governance principles, in turn, dictate what data will be sent to the Cloud and why. [4]

We use the term Information Governance very purposefully and differentiate it from mere information management. Information management fundamentally encompasses how information is created and flows through an organization. It is concerned mainly with infrastructure, applications and storage. Information Governance, on the other hand, concerns itself with why the information is created, used, and disposed of in the first place. Effective Information Governance requires an analysis by an organization to determine what information it needs to accomplish its objectives, the value of that information, and the period of time it will remain valuable.

Cloud Computing does not drastically change the principles of information governance, but it does add a layer of complexity. When an organization considers moving some or all of its information to the Cloud, it should consider all aspects of governance related to the collection, use, disclosure, transfer, modification, and disposition of that information, including:

. Data Creation: Create only information that is of value to the organization when weighed against any associated risk;

. Data Use: Ensure the availability of the information to those who need it;

. Data Security and Access: Secure the information from unauthorized access by those who do not need it; and

. Compliance Issues: Establish mechanisms to satisfy legal or regulatory obligations.

This may sound like a daunting task - and it does require assembling a consensus of disparate functional stakeholders - but an organization may find moving to a Cloud Computing environment provides an opportunity and incentive to enhance existing information governance policies and practices and to leverage newer technologies that may be available more economically in the Cloud than within a given enterprise. At the most fundamental level, **[*76]** an organization's data is a significant asset and should be managed like other important assets, pursuant to a governance structure, policies, and procedures aligned with the organization's objectives. But, as always, any such benefits should be appropriately weighed against the attendant risks addressed in this article and elsewhere.

A proper Information Governance structure requires an organization to solicit the perspectives of key functional stakeholders in the organization, including business leaders, legal, risk, compliance, human resources, records management, and IT. Each of these functional stakeholders brings valuable insight into the organization's objectives, duties and risks. The key to a successful Information Governance structure is understanding the

---

[4] The authors use the term "information" to refer to "electronic information," except where there is explicit reference to paper information, and will use the terms "information" and "data" (which is electronic information) interchangeably.

perspectives of each of these functional stakeholders, balancing their objectives and concerns, and establishing policies and procedures so that the organization creates, uses, and disposes of data in order to accomplish its objectives and fulfill its duties. [5]

An organization considering migration of its information to the Cloud should first determine the level of Information Governance structure it is able or willing to implement, and then evaluate a particular Cloud service and deployment model, as well as the specific Cloud Service Provider (CSP) that can help it do so. Organizations should also consider the potential level of disruption that migration of data to the Cloud could cause and take steps to minimize this disruption. An overall analysis may lead the organization to move some, but not necessarily all, of its information to the Cloud.

It is important to understand and assess how the chosen CSP facilitates the maintenance of data integrity and security prior to moving any data to the Cloud. [6] This assessment largely depends on an entity's objectives and its legal and regulatory obligations, and its risk profile and tolerance. There are **[*77]** a variety of laws and regulations establishing requirements and/or providing guidance in this area. [7]

Accordingly, organizations should be careful to understand how to create and govern the data, once migrated to the Cloud. Knowing this and other critical aspects about the information allows the organization to govern the information in compliance with its business objectives and its regulatory and legal obligations. The general considerations and standards discussed below are meant to provide guidance related to data (including metadata) governance in the Cloud. As we discuss more fully below, the CSP should be able to handle the incorporation and application of an organization's retention rules and other governance protocols. The basic hallmarks of even a rudimentary Information Governance system include, but are not limited to, mechanisms for these areas:

. Identifying who has access to information;

. Providing quick access to information;

. Ensuring the integrity of the information including its reliability, authenticity and usability for its intended life-cycle; and

. Reducing the costs associated with obsolete or duplicate records and information by providing for its disposition or destruction at the end of its life-cycle.

A. The Character of Cloud Data

---

[5] The Sedona Conference, Commentary on Finding the Hidden ROI in Information Assets 10-11 (2011).

[6] Entities should examine the extent to which the CSP can accommodate principles of records and information life-cycle management. This means that the entity should address the following through policies and procedures: who may create information, how it may be accessed, retrieved, modified (or modifications prevented), and how and when it may be destroyed or disposed. It should also consider the CSP-provided controls that are needed to ensure that the information is "trustworthy" (e.g., has integrity, is reliable). Having sufficient control over information is critical not only to proper Information Governance but, as we discuss more fully below, to properly conduct electronic discovery in the Cloud. Further, because organizations will want to avoid the e-discovery costs associated with keeping all information sent to the Cloud indefinitely, the absence of a disposition plan will undercut some of the economic benefits of moving to the Cloud, undermine the information management objectives of the data owner, and will likely conflict with data privacy obligations to maintain information no longer than necessary.

[7] See, e.g., Electronic Signatures in Global and National Commerce Act, *15 U.S.C. § 7001* (2000); *Fed. R. Evid. 901*; International Standards Organization, Information and Documentation--Records Management--Part 1: General, ISO 15489-1 (2001), available at *http://www.iso.org/iso/* catalogue_detail?csnumber=31908. See also DoD Records Management Program, No. 5015.2 (Dep't of Def. Mar. 6, 2000), available at *http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf*; The Generally Accepted Recordkeeping Principles - Generally Accepted, Specifically Relevant, ARMA Int'l, *www.arma.org/docs/sharepoint-roadshow/the-principles_executive-summaries_final.doc* (last visited Sept. 26, 2013); MoReq Collateral Website, *www.moreq1.eu* (last visited Sept. 26, 2013).

The determination of whether to send data to the Cloud starts with an examination of the subject data and the organization's needs for modalities of creation, storage, and disclosure. But first, the organization and the relevant stakeholders, from IT to Records to business owners to Legal, require an understanding of "the Cloud."

"Cloud Computing" refers to the on-demand access to computing services, such as applications, virtualized hardware, and storage, available via an Internet connection. A more technical definition is:
[*78]

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model [promotes availability and] is composed of five essential characteristics, three service models, and four deployment models. [8]

1. Does the Data Fall Under the Rubric of Domestic or International Privacy, Data Protection or Data Security Laws?

Electronic information storage and dissemination are affected by a myriad of laws and regulations, as discussed below. Preparatory to an analysis of the provisions that may affect the uses of an organization's data, the lawyer initially should have a grasp of the categories of issues to which the statutes and regulations, within the United States and across the globe, pertain.

[*79] While the specific legal and regulatory requirements concerning data storage will likely vary depending on the character of the data and the nature of the Cloud Consumer, the following examples serve as highlights:

---

[8] Peter Mell & Timothy Grace, Nat'l Inst. of Standards & Tech., U.S. Dep't of Commerce, Special Pub. No. 800-145, The NIST Definition of Cloud Computing 2 (2011), available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. The National Institute of Standards and Technology (NIST) is the federal technology agency that works with industries to develop and apply technology, measurements, and standards. Id. at ii.

Cloud Computing deployment models commonly include:

. The Public Cloud: Provided by a third-party and accessible to the general public with data typically secured and segregated among users or groups of users (typically no cost).

. The Private Cloud: Provided by a third-party for a fee allowing pooling of resources and/or eliminating resources as needed, and exclusive access only to those authorized to do so (i.e., employees).

. The Hybrid Cloud: Provided by a third-party, allowing access to a combination of a Public and Private Clouds, allowing, for example, the use of a Public Cloud for email and a Private Cloud for more sensitive documents and/or databases.

Id. at 3.

Cloud Computing "Service Models" generally include the following:

. Software as a Service ("SaaS"): The CSP manages the underlying infrastructure and provides access to software applications or programs via "thin client interfaces" over Internet web browsers with little to no ability to customize (e.g., SalesForce.com, CaseCentral.com, etc.).

. Infrastructure as a Service ("IaaS"): IaaS provides the most flexibility of all of the service models. IaaS provides outsourcing of equipment or hardware to support I.T. functions with the Cloud user controlling the applications available to it, but not the capability to modify and manage essential computing resources, operating systems, storage, networking components, and firewall hosting (e.g., Amazon Web Services, RackSpace, GoGrid, Nirvanix).

. Platform as a Service ("PaaS"): PaaS is similar to IaaS except the CSP typically manages the underlying infrastructure such as the configuration and maintenance of operating systems (e.g., Windows Azure, Force.com, and Google App Engine).

Id. at 2-3.

. Data Security: Includes issues of encryption and other forms of safeguards (i.e., passwords and other forms of access authorization for data in storage and in transit to and from a CSP; security breach, disaster recovery, and interruption of power or Internet connectivity, data encryption (inalterability)), as well as a clear understanding of the need for and access to data by CSP personnel and what happens in the event of the demise of a CSP.

. Physical Location and Security of Data: Includes an understanding of where the CSP may hold the information (e.g., single or multiple dedicated data centers, geographic location, etc.), as well as the on-premise security of buildings, servers, etc.

. Data Classification: Includes how the CSP handles security classifications for information within specific Cloud Computing environments, e.g., "company private," "confidential" or "secret," and "top secret."

Some practical and technical aspects of data security may favor the use of Cloud Computing over the traditional model of entity-owned data center(s). For instance, CSPs can employ security processes and protocols that may be beyond the means of many small entities. These security protocols can include not only the storage and transmission of information, but also physical security measures and administrative protocols.

Other characteristics of Cloud Computing make the Cloud especially useful in securing information simply because of the way Cloud data is stored. For example, a CSP may replicate data across multiple servers, and it is unlikely that all of those servers will fail at the same time or that an unauthorized user could gather all of the pieces of a distributed file without detection. However, this replication across multiple servers (and perhaps jurisdictions) can also create potential security and legal risks. More pieces of files in more locations means the pieces may frequently be in transit, through servers where security may be less robust, and over which a CSP may have less control. Data traveling through certain jurisdictions may come under the control of those jurisdictions' privacy provisions, laws, or other regulations regarding security of protected data.

Another Cloud Computing characteristic that may enhance security is that CSPs usually have hundreds or thousands of servers that they can employ to host and route data. In a traditional computing model where an entity's data is on servers owned or possessed by it, if a server fails or is **[*80]** compromised, the entity may need to take the server off-line, potentially leading to significant downtime. Replication of data in the Cloud can mitigate these problems. End users may thus experience little to no loss of data access and may benefit from faster restoration of data.

2. Does the Location of Data on Servers Outside the United States Affect Access to the Data or the Ability to Transfer and Disclose It as Needed?

Jurisdiction has traditionally been based on the physical location of the res, the thing at issue. [9] Cloud data may be present in several places at once, but inquiry often begins with the location of the servers on which the data resides. CSPs can develop systems, processes, and protocols that comply with legal obligations in privacy and/or security, as required by various United States statutes. [10] In addition, the European Union Data Protection Directive and implementing statutes prohibit the disclosure of personally identifiable information (PII) to jurisdictions that do not meet minimum standards, including the United States, unless certain safeguards are in place. [11] CSPs may enable

---

[9] See, e.g., *Shaffer v. Heitner, 433 U.S. 186, 207 (1977)*.

[10] See, e.g., Dodd-Frank Wall Street Reform and Consumer Protection Act, ***Pub. L. No. 111-203***, ***124 Stat. 1376*** (codified as amended in scattered sections of 7 U.S.C., 12 U.S.C., 15 U.S.C., 18 U.S.C., *22 U.S.C., 31* U.S.C. & 42 U.S.C.); Sarbanes-Oxley Act of 2002, ***Pub. L. No. 107-204***, ***116 Stat. 745*** (codified as amended in scattered sections of 15 U.S.C. & 18 U.S.C.); Health Insurance Portability and Accountability Act of 1996, ***Pub. L. No. 104-191***, ***110 Stat. 1936*** (codified as amended in scattered sections of 18 U.S.C., *26 U.S.C., 29* U.S.C. & 42 U.S.C.); Privacy and Security, Fed. Trade Comm'n, available at *http://www.business.ftc.gov/privacy-and-security*; FINRA Rules, Fin. Indus. Reg. Auth., Inc., *http://www.finra.org/Industry/Regulation/FINRARules/* (last visited Sept. 26, 2013); Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, PCI Security Standards Council, L.L.C. (Oct. 2010); SEC Final Rules, U.S. Sec. & Exch. Comm'n, *http://www.sec.gov/rules/final.shtml* (last updated Aug. 21, 2013).

compliance with these provisions by situating the subject data on servers within the European Union, or a specific country - either physically or virtually. The FTC has created a "Safe Harbor" certification program whereby an entity meeting the European Union's **[*81]** security requirements can receive PII regarding European Union citizens. [12] CSPs that meet these requirements may be able to provide this compliance benefit to its users. [13]

3. Cross-Border Concerns: Storage and Transfer of Cloud Data

One issue of special concern to Cloud users is the location of information when it is stored as well as information in transit. In particular, a Cloud user should pay special attention to whether information moved to the Cloud is being stored in a jurisdiction outside the United States that imposes restrictions on the transfer or disclosure of that information. [14] The converse is also true - Cloud users in the European Union and other countries with data restrictions should be alert to the storage of information outside of those countries unless they have implemented sufficient protections. Some of these protections include complying with the Safe Harbor self-certification rules promulgated by the U.S. Department of Commerce and International Data Transfer Agreements based upon Model Clauses promulgated by the E.U. Data Privacy Commission, or the establishment of Binding Corporate Rules. [15]

In some circumstances, however, it may be difficult for a Cloud user to know the physical location of its information in the Cloud, depending on the service and deployment model and the specific contractual agreements between the CSP and the user. Some CSPs will agree to restrict the location of a user's information to a specific jurisdiction as well as restrict the routing of information through certain jurisdictions. As with the other aspects of Cloud Computing discussed in this Commentary, it is critical that entities consciously consider, discuss, and negotiate these issues, to the extent possible, with the CSP prior to making a decision to move information to the Cloud so that it may fully understand the risks and benefits of such a move. If it determines to move information to the Cloud, it should develop Information Governance policies and implementing procedures specifically tailored to the strengths and weaknesses of the particular Cloud offering.

[*82] Location of data stored in the Cloud can raise thorny jurisdictional issues. In the Cloud environment, even determining where data is located may be complex. In eBay Canada, Ltd. v. Minister of National Revenue, the Minister of Revenue of Canada sought information on Canadian eBay "Power Sellers" for purposes of determining tax liability. [16] The court found jurisdiction, despite the fact that many of the parties to the transactions - as well as much of the data - were outside Canada: "[The] information cannot truly be said to "reside' only in one place … [it is] instantaneously available." [17] The law regarding jurisdictional aspects of Cloud data is especially nascent and conflicting. Therefore, an organization considering a move to the Cloud should fully understand where its data will

---

[11] See Council Directive 95/46, 1995 O.J. (L 281) (EC) [hereinafter EC Privacy Directive], available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en*: HTML. In 2012, a significant revision of the EC Privacy Directive was proposed. See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), available at *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*.

[12] U.S.-EU & U.S.-Swiss Safe Harbor Frameworks, Export, *http://export.gov/Safeharbor/* (last visited Sept. 26, 2013).

[13] See, e.g., The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts: A Partial Guide to Navigating the Competing Currents of International Data Privacy and E-Discovery 27-28 (2008) [hereinafter Sedona Framework], available at *https://thesedonaconference.org/publication/Framework%20for%20A* nalysis%20of%20Cross - Border%20Discovery%20Conflicts.

[14] See EC Privacy Directive, supra note 11.

[15] See Sedona Framework, supra note 13.

[16] e Bay Canada Ltd. v. Minister of Nat'l Revenue, [2007] F.C. 930 (Can. Fed. Ct.).

[17] Id. at 13.

be stored and through which jurisdictions it will transit and assess any associated risks prior to moving any data to the Cloud.

4. United States Privacy Considerations

There is no general national privacy law in the United States, but privacy laws exist at the federal level in three areas: healthcare, finance, and education. [18] The protected nature of such data implicates the privacy, security, and integrity of Cloud information, and accordingly, may require the data owner to assure that the Cloud provider safeguard the data in accordance with pertinent law and regulations. For example, storage of certain patient-identifiable data ("Protected Health Information," or "PHI") with a CSP, without encryption, is a "disclosure," and disclosures cannot be made without authorization of the data subject to the patient or proxy, unless the disclosure falls within the exceptions in the Privacy or Security Rule. [19] Many healthcare providers and health insurance plans, therefore, opt to send only encrypted PHI to the CSP and will not provide the Cloud entity with the decryption key. One of those disclosure exceptions permits the disclosure of PHI to "Business Associates" such as CSPs if the healthcare plan or provider has entered into a Business Associate Agreement, by which the Associate, **[*83]** the CSP here, agrees to protect and maintain the PHI in accordance with certain provisions of the HIPAA Privacy and Security Rules. [20]

State laws may require specific provisions in the Cloud SLA in order to comply with privacy and data protection laws. For example, Massachusetts' Standards for the Protection of Personal Information of Residents of the Commonwealth require compliance with certain levels of technical safeguards for those, including CSPs, who hold and use personal information of Massachusetts citizens. [21] These safeguards include encryption and administrative protocols (policies and procedures) such as access and authorization controls. [22] The entity that sends such personal data to a CSP would be well advised to read these Regulations carefully, and also research similar regulations of other states whose citizens' data may be the subject of an SLA. [23]

5. Who Owns Data in the Cloud? The Transferring Entity? The CSP? Both? What does the CSP Contract, or Service Level Agreement ("SLA"), Say?

Traditional notions of possession, custody, and control do not always easily translate to the storage model of Cloud Computing. A key area of concern relates to data ownership and access. For instance, an SLA that explicitly states that the client owns all data transferred to or created in the Cloud, and that the SLA is binding on the CSP and its successors and assigns, may reduce or avoid issues that could arise if the CSP enters bankruptcy proceedings, or if the Cloud user needs access to electronically stored information ("ESI") that is stored in the Cloud in order to preserve or collect it. Clearly addressing these types of issues in the SLA may reduce the chance a CSP would refuse to allow sufficient access rights to the user to enable it to comply with its e-discovery and other obligations. This is also pertinent to non-litigation matters, such as regulatory compliance (i.e., Second Requests from the U.S. Department of Justice or the Federal Trade Commission with regard to approval of mergers), or in due diligence analyses during a merger, sale, or acquisition.

---

[18] See, e.g., Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999), *15 U.S.C. § 6801* (2006); Family Educational Rights and Privacy Act, *20 U.S.C. § 1232g* (2006); Health Insurance Portability and Accountability Act of 1996, ***Pub. L. No. 104-191***, ***110 Stat. 1936*** (codified as amended in scattered sections of 18 U.S.C., *26 U.S.C., 29* U.S.C., and 42 U.S.C.); ***45 C.F.R.§§160.103***-.552 (2013).

[19] ***45 C.F.R. § 164.502***.

[20] See *45 C.F.R. § 164.504*.

[21] 201 Mass. Code Regs.§§17.01, 17.04 (2013).

[22] Id.

[23] Cf. *Cal. Civ. Code §§56.10*-16 (West 2013) (personally identifiable medical information of California residents subject to California's Confidentiality of Medical Information Act).

While some organizations may be able to negotiate an SLA that expressly addresses e-discovery and disclosure obligations, others may not **[*84]** have the market power to do so. A growing number of organizations use free Cloud services, such as Gmail, to store information and communicate with others. [24] Many of these services are governed by Standard Terms of Service ("TOS") agreements in SLAs that are often non-negotiable or subject to change. Thus, it is important for an organization to understand precisely what the CSP will and will not do with respect to these issues so that it may appropriately weigh the benefits and risks prior to moving to the Cloud.

As the number of customers and providers in the Cloud economy increases, the challenges of control, access, and ownership will grow in tandem. The SLA used by the party contracting for Cloud services should consider and, if possible, address these complexities, which may then be understood and interpreted, much of the time, under established principles of contract law.

B. Possession: Who Has Control and Access, and How Is the Data Controlled/Accessed by the Cloud Customer and CSP?

Obtaining data from the Cloud for legal or regulatory purposes implicates a myriad of technical and legal issues, so it is imperative that Cloud Customers think through - and negotiate where feasible - how they can access and extract data from the Cloud. Cloud Customers are responsible for knowing where and how to access their data, and in what format the data will be extracted, for whatever the reason (e.g., data management and self-collection tools, APIs, vendor options, etc.). These processes can take significant time, create expense, and impact entities' business functions. Thus, it is critical to assess this prior to contracting with CSPs. While accessibility, burden, and costs are legitimate arguments in response to legal or regulatory demands, housing data in the Cloud will not protect Cloud Customer litigants from having to comply with their obligations to produce relevant data, etc. Cloud Customer entities prepared with the above knowledge can utilize such in complying with, for instance, obligations pursuant to *Federal Rules of Civil Procedure 26* and *34*, as discussed infra.

Generally, relevant, accessible, and non-privileged ESI in a responding party's possession, custody, or control is discoverable, regardless of where it **[*85]** is stored. [25] When entities place ESI in the Cloud, they should be cognizant of and anticipate issues that might develop when legal obligations arise. [26] Entities cannot simply claim that storing data in the Cloud deems it "inaccessible" in terms of legal obligation. [27]

In a traditional computing model, a party usually has physical possession or custody of most of its ESI. But in a Cloud Computing model, the ESI is generally under the physical control of the CSP. The discovery obligation analysis should not, however, be overly complicated by the fact that physical possession, custody, and control may be split between the responding party subject to discovery obligations and a third-party CSP (or several) not

---

[24] See *Oregon v. Bellar, 217 P.3d 1094, 1110 (Or. Ct. App. 2009)* (Sercombe, J., dissenting) (concluding that "our social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the "cloud,' on servers owned by internet service providers"); Rachael King, How Cloud Computing is Changing the World, Bloomberg Businessweek, Aug. 4, 2008, *http://www.businessweek.com/stores/2008-08-084/how-cloud-computing-is-changing-the-worldbus* inessweek-business-news-stock-market-and-financial-advice (estimating that the annual global market for Cloud computing will be $ 95 billion by 2013).

[25] *Fed. R. Civ. P. 26*.

[26] *Fed. R. Civ. P. 34(a)(1)* (allowing a party involved in litigation to request discovery of ESI in the responding party's "possession, custody, or control"). See *Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (D. Md. 2010)* (discussing law of various circuits); *The Sedona Conference Commentary on Legal Holds: The Trigger & the Process, 11 Sedona Conf. J. 265 (2010)*; The Sedona Conference Commentary on Non-Party Production & Rule 45 Subpoenas (2008) (detailing the discussion of parties' and third parties' e-discovery obligations). See also The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production 48 (2d ed. 2007) (comment 8.d).

[27] See Columbia Pictures v. Bunnell, No. 2:06-cv-*01093 FMC-JCx, 2007 U.S. Dist. LEXIS 96360, at 20-21 (C.D. Cal. 2007)* (rejecting the claim that data in Netherlands was inaccessible because of Netherlands privacy laws).

involved in the litigation. As discussed below in the section on e-discovery, the Cloud customer, while not in physical possession of all of its ESI all of the time, has the duty to preserve and produce such ESI. Accordingly, it is the practical responsibility of the Cloud Customer to secure vendors able to extract Cloud data and/or understand the CSP tools available for such data extraction when needed.

C. Subpoenas, Government Agency Demands, and Civil Discovery Requests

In the traditional computing model, discovery requests are made under *Federal Rule of Civil Procedure 34* for data subject to discovery pursuant to Rule 26, and data are produced from servers or individual devices by various means. But in a Cloud computing model, a party to litigation or a governmental entity may seek the data either by a Rule 34 request to the Cloud user or via a Rule 45 or other subpoena directly to the CSP. [28] As discussed in the previous section, because the data is under the control of the Cloud user, the user can obtain the data from the CSP in order to respond to the Rule 34 request or subpoena. But with Cloud Computing, the CSP may be the subject of a civil subpoena, government agency demand, or a **[*86]** governmental subpoena directly. This adds a layer of complexity - especially concerning the Stored Communications Act discussed infra - and, absent careful analysis and attention during the contracting documentation phase of arranging for Cloud Computing, risk to the discovery process.

While there are relatively few court decisions specifically addressing Cloud Computing, there are opinions that address the more general, yet applicable, circumstance in which a third party possesses a litigant's ESI. A number of courts have ruled, over a period of many years, that ESI held by a third party on behalf of a litigant and/or its law firm lies within the party's control. [29] Thus, if a party has the practical ability or legal right to obtain the ESI on demand, or has retained any right or ability to direct the third party that holds the ESI, courts have concluded that the party has control of it for purposes of the discovery rules. [30]

In Zynga Game Network, Inc. v. McEachern, [31] the defendant was sanctioned and ordered to direct a computer rental vendor to turn over previously rented servers so that the plaintiff could access those servers and copy their contents. [32] With little analysis, the court determined that those servers were within the control of the party that

---

[28] See *Fed. R. Civ. P. 45*.

[29] See, e.g., *Tomlinson v. El Paso Corp., 245 F.R.D. 474, 476-77 (D. Colo. 2007)*; *Starlight Int'l v. Herlihy, 186 F.R.D. 626, 635 (D. Kan. 1999)*; *Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1426-27 (7th Cir. 1993)*; *Goodman v. Praxair Servs., Inc., 632 F. Supp. 2d 494, 516 n.11 (D. Md. 2009)*; *In re NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007)*; *Golden Trade, S.r.L. v. Lee Apparel Co., 143 F.R.D. 514, 525 (S.D.N.Y. 1992)*.

[30] *Flagg v. City of Detroit, 252 F.R.D. 346, 354-55 (E.D. Mich. 2008)* (relying on defendant's argument that its consent was required under the Stored Communications Act for disclosure of text messages in finding that defendant had control over the messages); Babaev v. Grossman, No. CV03-5076 (*DLI)(WDW), 2008 WL 4185703, at 3 (E.D.N.Y. Sept. 8, 2008)* (holding defendants had sufficient control over their bank records to obtain them); Tetra Techs., Inc. v. Hamilton, No. CIV-07-1186-*M, 2008 WL 3307150, at 1 (W.D. Okla. Aug. 7, 2008)* (holding that the user of the cell phone service had the legal right to obtain the cell phone records from service provider); *Tomlinson, 245 F.R.D. at 476-77* (stating that where third-party vendor had possession, custody and control of the electronic data, defendants could not delegate their statutory obligations to preserve and maintain data and avoid discovery); *In re NTL, Inc. Sec. Litig., 244 F.R.D. at 195* (finding that defendant had the practical ability to obtain any documents it needed from a third-party corporation); *A. Farber & Partners, Inc. v. Garber, 234 F.R.D. 186, 189-90 (C.D. Cal. 2006)* (ordering defendant to sign consent forms to release his documents from third parties including Nextel, Pacific Bell, banks, Internal Revenue Service, and California Franchise Tax Board).

[31] *Zynga Game Network, Inc. v. McEachern, No. 09-1557, 2009 U.S. Dist. LEXIS 39417 (N.D. Cal. Apr. 24, 2009)*.

[32] Id. at 5-6.

rented them, even after they were returned to the vendor, and no contractual relationship existed between the vendor and the defendant. [33]

[*87] These opinions demonstrate that the legal analysis courts have employed in determining whether ESI is under a party's "control," and thus discoverable under the Federal Rules, including the broad "practical ability" test, [34] is unlikely to change when the party employs a Cloud-computing model for storing ESI.

1. Subpoenas Served on the Cloud Customer

These opinions demonstrate that the entity whose information is hosted by a CSP will be deemed to have legal control over that information in virtually all cases. Thus, when served with a Rule 34 discovery request, a Rule 45 subpoena, or a government subpoena seeking data held in the Cloud, the entity would respond just as it would to similar requests and subpoenas when it is in possession of the data in its data centers.

The Stored Communications Act ("SCA"), discussed infra, governs when and how a CSP may respond to a civil or criminal subpoena. [35] The Cloud Customer should negotiate with the CSP for timely notification of receipt of a subpoena for its data, subject to provisions of the SCA. This would provide the Customer with the opportunity to object to the disclosure and, where appropriate, prepare a motion to quash the subpoena. Refusal of the CSP to consider such notification adds an additional level of risk to be assessed prior to moving data into the Cloud.

Likewise, to the extent the CSP has Cloud Customer data located across the globe within various data center locations, the identification and collection of such data could trigger cross-border issues, which would otherwise not exist if the Cloud Customer maintained its own data centers. [36] Consequently, the party has an obligation to identify, collect, review, and produce relevant ESI in the possession of its CSP, unless it is protected or if it can prove the data is inaccessible because of undue burden or cost. [37] It is essential, then, for the entity to understand precisely how ESI can be **[*88]** produced from the Cloud and the burden of doing so before it moves its data to the Cloud.

2. Subpoenas Served on the CSP

A CSP may be subpoenaed directly by a party (or the government) seeking the information of the Cloud Customer. As discussed in the previous section, because the information is usually under the control of the entity, the entity can obtain the information from the CSP in order to respond to the Rule 34 request or subpoena. But with Cloud Computing, the CSP is in possession of an entity's information and is now subject to a Rule 45 or other subpoena or a government demand or subpoena directly, with some limitations imposed by the SCA. [38]

---

[33] The court did not consider the question of whether the servers would have been within the defendant's control if they had been rented again and resided with another renting party. Id.

[34] See, e.g., *Tomlinson, 245 F.R.D. at 476-77*.

[35] *18 U.S.C. § 2701* (2012).

[36] Cf. Columbia Pictures, Inc. v. Bunnell, 2:06-cv-*01093 FMC-JCx, 2007 U.S. Dist. LEXIS 96360, at 24-25 (C.D. Cal. Dec. 13, 2007)* (rejecting claim data could not be produced because they were housed with a Netherlands CSP); British Columbia Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, P.30.1 (Can.), available at *http://www.bclaws.ca/EPLibraries/* bclaws_new/document/LOC/freeside/%20F%20/Freedom%20of%20Information%20and%20Protection%20of%20Privacy%20Act%20RSBC%201996%20c.%20165/00_Act/96165&uscore;03.xml#section30.1 (personal information to be stored within Canada).

[37] See *Fed. R. Civ. P. 26(b)(2)(B)*.

[38] *18 U.S.C. § 2703* (2009).

The SCA further complicates subpoena issues in the Cloud Computing environment. The SCA was passed in 1986 and addresses technology as it existed at the time, using terms applicable to that technology, but that are outdated and inaccurate in addressing today's technology. An effort to update the SCA has been sponsored by Senator Patrick Leahy (D-VT), and committee hearings may commence in 2013. [39]

A CSP is a provider of an electronic communications service ("ECS") - and thus covered by the SCA - if it allows one to send or receive wire or electronic communications. [40] Wire communications transmit a human voice, such as telephonic voice mail, while electronic communications, such as email or text messages, do not. [41] An ECS provider may not knowingly divulge the contents of any communication while it holds the communication in electronic storage. [42]

A CSP may also be the provider of a remote computing service ("RCS") if it provides computer storage or processing that uses an electronic communications system to the public. [43] An RCS may not divulge the contents of a communication that the RCS holds in storage for the subscriber or customer that was received electronically from that subscriber or **[*89]** customer, and if the communication is held solely for the purpose of providing the RCS service to the subscriber or customer. [44]

A CSP can be an ECS, an RCS, or both. Because these terms are defined very broadly, virtually every deployment and service model is covered by the SCA. Case law interpreting the SCA has consistently held that an ECS/RCS may not divulge the contents of a communication even when served with a Rule 45 subpoena because there is no exception in the SCA to allow it. [45] Thus, even when a CSP is served with a Rule 45 subpoena, it often does not have to divulge the contents of stored communications, and if it does, it violates the SCA with potentially serious liability. [46]

The definition of an electronic communication is very broad - "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce" [47] - and conceivably covers the contents of virtually any sort of information held by a CSP. However, the SCA does not protect the disclosure of the existence of a communication or the parties to it. [48] It is possible that artful counsel could develop discovery strategies that seek useful information from a CSP that does not divulge the contents of a communication (such as records about the kinds and volumes of data stored, contract terms, lists of custodians, etc.). Thus, it is important that an entity fully understand what non-content information is created by, and available from, the CSP in considering whether to move information to the Cloud.

---

[39] Press Release, Sen. Patrick Leahy, On Introduction of "The Electronic Communications Privacy Act Amendments Act of 2013" (Mar. 19, 2013), available at *http://www.leahy.senate.gov/* press/leahy-lee-introduce-legislation-to-update-electronic-communications-privacy-act.

[40] *18 U.S.C. § 2711* (2009).

[41] See id.

[42] Id. § 2702(a)(1).

[43] Id. § 2711(2).

[44] Id. § 2702(a)(2).

[45] See, e.g., *United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)*. See also *18 U.S.C. § 2702(a)* (2008) (stating that a provider shall not divulge the contents of the communication).

[46] See Id. §§2701(b), 2707(b)-(c).

[47] Id. § 2510(12).

[48] See Id. § 2702(a) (stating that a provider shall not divulge the contents of the communication).

While the protections of the SCA seem quite broad, they are also somewhat ephemeral. This is because the SCA allows the CSP to divulge the contents of communications with lawful consent. [49] This consent can come from the Cloud user, among others. [50] An increasing number of cases hold that if the user is subject to a Rule 34 discovery request, that user must provide consent to the Provider to divulge the contents of the communications. [51] Thus, the party that seeks discovery from a CSP could **[*90]** simultaneously serve a Rule 34 request to the user and a Rule 45 subpoena to the CSP, and likely obtain any relevant discovery that it seeks. Because of this, it is critical that an entity fully understand how ESI can be identified, preserved, and collected from the Provider, and at what cost, before moving information to the Cloud.

Many potentially problematic issues can be addressed when negotiating an agreement with a CSP (if such negotiations are possible) including:

. A CSP's obligation to notify the entity upon receipt of a subpoena (e.g., Rule 45) and/or court order. Sufficient notice allows for the entity to assert and protect its rights. As discussed more fully below, notice can become complicated, however, when the subpoena is issued as part of a criminal investigation, because that part of the Electronic Communications Privacy Act *18 U.S.C.§§2701-2712* (ECPA) prevents the Provider from notifying the entity in certain cases, at least for some period of time;

. CSPs can also be served with process by state officials and under state law. CSPs are obligated to produce;

. Cloud data stored in data centers across the world may also subject Cloud Customers to unexpected international issues and potential obligations by sovereign law enforcement processes served on CSPs;

. The steps the Provider will/must take (and will not take) in response to a subpoena; and

. The costs associated with responding to a subpoena and how such costs will be apportioned.

D. How Is Discovery of Cloud Data Obtained?

In many ways, e-discovery in the Cloud is not very different from traditional e-discovery. An entity is ultimately responsible for responding appropriately to litigation discovery requests. Among other things, this means being able to identify information potentially relevant to the litigation and preserve, collect, review, and possibly produce it. But while these obligations are not new, fulfilling them can be very different in the Cloud. One of the issues with Cloud Computing is that a Customer's data is now under the direct control of a third party and, perhaps, in scattered locations **[*91]** unknown to the Customer. This has implications regarding custody and control, vulnerability to subpoenas, and liability for data loss, among other things. Another issue to be aware of is that the nature of Cloud Data means there is more of it. For instance, Cloud data is often automatically saved as it is created; thus, not only is the document saved, but the revisions to the document (i.e., email, documents, spreadsheets, etc.). CSPs handle this issue in different ways, so it is critical to understand their process and how it will impact data collection, segregation of drafts from the documents, etc. Finally, Cloud-provided collaborative work environments, while terrifically efficient, also create new notions of what a document is. Now, there is one document and many contributors, unlike many unique versions of the document (i.e., Microsoft Word). This issue not only impacts e-discovery collection, but retention and deletion of documents. The discussion below explores these issues and the concepts that should be considered when addressing them.

---

[49] Id. § 2702(b)(5).

[50] Id. § 2702(b)(3).

[51] See, e.g., *Flagg v. City of Detroit, 252 F.R.D. 346, 355 (E.D. Mich. 2008)*; Columbia Pictures Indus. v. Fung, No. CV 06-*5578 SVW(JCX), 2007 U.S. Dist. LEXIS 97576, at 30-31 (C.D. Cal. June 8, 2007)*; Columbia Pictures Indus. v. Bunnell, No. CV 06-*1093 FMC(JCx), 2007 U.S. Dist. LEXIS 46364, at 14 (C.D. Cal. May 29, 2007)*.

1. Can Cloud Data Be Preserved as Required by Law? Information Management, Identification and Preservation, and Legal Holds

Preservation and/or collection of ESI, whether self-collected or vendor assisted, is fundamentally different from preservation and collection from the entity's own servers and devices. To the extent a CSP cannot technically implement an entity's existing policy/practice for data retention and preservation, the entity may have to adjust its policies and/or preservation practices to ensure compliance with any legal obligations. These issues, as well as how the CSP will work with the entity or its vendor to ensure collection of all relevant data, including a comprehensive understanding of back-up and redundancy practices, metadata types, and retention processes, should be addressed prior to contracting for Cloud services when possible.

A party has a duty to preserve information relevant to an issue when it is reasonably foreseeable that the issue is or will be the subject of litigation. [52] Yet, when an entity places its information in the Cloud, fulfilling its duty to preserve data in the hands of the third-party and the ability to defend its means of doing so, adds additional challenges. It is advisable to address preservation issues in the Terms of Service or SLA. In addition, the party should understand precisely what protocols the CSP will undertake to preserve metadata, and what degree of access the user will have to **[*92]** identify, collect, and export metadata to satisfy its e-discovery and disclosure obligations. [53]

When faced with reasonably anticipated litigation, entities typically identify individuals (or custodians) who had some relation to the issues involved in the litigation, identify the information they might have created or possess regarding those issues, and preserve that information via "litigation hold." This is also true of sources of information not specifically related to a particular custodian, but that also might be relevant, such as databases or collaboratively created documents. In the traditional computing model, entities can identify and preserve information associated with custodians fairly easily: they usually have an email account, a local computer, and space on a network drive to which they have access.

In Cloud Computing, implementing a litigation hold may be more challenging. The preservation steps that a particular CSP can or is willing to take will vary. [54] Some CSPs have tools that allow the Cloud Customer to manage its own data for information governance, compliance, and other legal matters, while other CSPs provide Application Programming Interfaces (APIs), allowing Cloud Customers to work with their own internal I.T. departments and/or vendors to export the requisite data. Regardless of the specific process provided by the CSP, it is critical that the Cloud Customer understand specifically what the CSP will and will not do in order for it to properly evaluate the risks of moving information to the Cloud.

2. Spoliation and Sanctions - Does Data in the Cloud Have an Impact?

With potentially critical information in the hands of a third-party and the information owner nevertheless responsible for its integrity, spoliation is a serious concern. Loss of information can result in various forms of sanctions and other negative consequences imposed by a court under applicable statutes or rules or pursuant to the court's

---

[52] See, e.g., *In re NTL, Inc. Sec. Litig., 244 F.R.D. 179, 193 (S.D.N.Y. 2007)*.

[53] See David D. Cross & Emily Kuwahara, E-Discovery and Cloud Computing: Control of ESI in the Cloud, Elec. Discovery & Digital Evidence J., Spring 2010, available at http://www.american bar.org/content/dam/aba/administrative/science_technology/edde_journal_volume_1_issue_ 2.authcheckdam.pdf.

[54] Collaborative documents pose a particular issue regarding litigation hold. When there is one document and many potential contributors/collaborators, placing one collaborator on litigation hold effectively means placing all collaborators on hold. Companies must assess the risk of this and determine what process is most effective for collection in a particular matter. Likewise, previous versions of the document(s) are saved and will need to be segregated and/or collected depending on the negotiated ESI agreement in the matter.

inherent authority. These may **[*93]** include terminating sanctions, preclusion of evidence, adverse inferences, awards of costs or fees, or additional discovery. [55]

Yet, courts thus far have been inconsistent in assessing levels of culpability that can give rise to sanctions. In Pension Committee, the court attempted to provide guidance as to what discovery conduct and preservation practices may be considered, by holding that the degree of culpability resulting in data loss determines the level of prejudice and, therefore, sanctions. [56] This holding, however, has been met with some criticism. [57] The court in Rimkus [58] took a different approach, finding that, while defendants had participated in intentional spoliation of evidence, terminating sanctions were inappropriate because the plaintiff was unable to show a sufficiently high degree of resulting prejudice; that is, the subject information's absence did not rise to the level warranting termination, regardless of the conduct involved in that loss.

In Orbit One Communications, the Second Circuit backed away from the holding in Pension Committee, which focused primarily on the culpability of the spoliator and inferring relevance and prejudice thereby. Instead, the court stated that "rather than declaring that the failure to adopt good preservation practices is categorically sanctionable, the better approach is to consider such conduct as one factor … and consider the imposition of sanctions only if some discovery-relevant data has been destroyed." [59]

Even though the Orbit One court sought to establish several factors to be considered in determining the award of sanctions, the issue continues to be debated. Recently, Judge Scheindlin in the Southern District of New York issued yet another opinion analyzing how an aggrieved party can prove relevance and prejudice from spoliated (and therefore missing) information. In Sekisui Am. Corp. v. Hart, [60] the court held that relevance and, therefore, **[*94]** prejudice could be assumed because of the role or function of the person whose data was spoliated.

Courts continue to hold parties to differing standards, depending on the jurisdiction. But even with these variations, the finding of sanctionable conduct is fundamentally a fact-specific inquiry, with the most important factors being the reasonableness of the responding party's conduct (both before and during litigation) and the degree of prejudice to the requesting party. [61] The more diligence an entity can show it undertook in considering a move to the Cloud, and by implementing contractual terms and protocols aimed at preventing the loss of relevant data, the entity can significantly reduce the chance that it will face serious sanctions for spoliation if it does occur.

Cloud data potentially presents different issues to a general spoliation analysis. Factors, such as (1) possession, custody, and control; (2) implementation of reasonable holds; and/or (3) intent, come into play. In this regard, the spoliation analysis may differ if the owner failed to have sufficient control over the data when the data was lost; the owner failed to take reasonable steps to ensure the CSP was on notice of the obligation to preserve or to work with the CSP to ensure the data was preserved; and the intent of the data owner, as opposed to the provider, displayed

---

[55] See *Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 533 (D. Md. 2010)* (discussing sanctions available to a federal court). The severity of sanctions that may be levied upon a party found to have spoliated Cloud data may vary with the jurisdiction and the degree of culpability of the infringing party and prejudice to the complaining party. *Id. at 542-53*.

[56] See *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., L.L.C., 685 F. Supp. 2d 456 (S.D.N.Y. 2010)*, overruled on other grounds by *Chin v. Port Auth. of N.Y. & N.J., 685 F.3d 135, 162 (2d Cir. 2012)* ("We reject the notion that failure to institute a litigation hold constitutes gross negligence per se.").

[57] *Id. at 468-71*.

[58] *Rimkus Consulting Grp., Inc. v. Cammarata, 688 F. Supp. 2d 598, 644-45 (S.D. Tex. 2010)*.

[59] *Orbit One Commc'ns, Inc. v. Numerex Corp., 271 F.R.D. 429, 441 (S.D.N.Y. 2010)* (emphasis added) (citation omitted).

[60] *Sekisui Am. Corp. v. Hart, No. 12 Civ. 3479, 2013 U.S. Dist. LEXIS 115533 (S.D.N.Y. Aug. 15, 2013)*.

[61] See, e.g., *Rimkus, 688 F. Supp. 2d at 613-20*.

in the loss of the data (i.e., should the owner be punished where it undertook reasonable steps, but the data was lost as a result of the CSPs' wrongful conduct?). Courts long have held that a party may be held responsible for the spoliation of information, not through their own actions, but due to the conduct of their agents, which would include third-party CSPs. [62]

Whether a party conducted reasonable due diligence prior to storing information in the Cloud may be a factor in a spoliation determination. For instance, if the CSP has sub-contracted with others, a chain of due diligence may be required. Thinking about and addressing these issues in advance, as well as documenting decisions regarding them, could well be seen to minimize risk upfront and may provide the foundation for defending the reasonableness of an entity's conduct.

An entity should also understand the steps the CSP will take in response to a specific matter, and the entity should carefully document each step it **[*95]** takes in the discovery process in case of subsequent challenge. Likewise, an entity and the CSP should consider and contractually address issues related to spoliation liability for loss of information. The SLA, to the extent possible, should establish clearly delineated obligations, provide a mechanism for placing and implementing legal holds on stored data, and define penalties and indemnification rights. It may also be a good idea to try to address the disposition of Cloud data (i.e., the process of data disposal) and who bears the risk, if any, should the data be inadvertently kept beyond the agreed-upon retention schedule(s), thus making such data potentially discoverable.

Determinations of liability for spoliation of information in the Cloud are not that different than those involving any potential destruction of information - was the data identified at the outset (i.e., during Rule 26(a)(1) disclosures), and when the duty to preserve was triggered, was the Cloud data preserved and/or purge practices suspended in a reasonable manner, etc.? To the extent that reasonable steps are followed, yet spoliation occurs, questions may focus on the terms of the contract for Cloud Services and whether aspects related to preservation and collection of information were negotiated up front. Inevitably, "each case will turn on its own facts and the varieties of efforts and failures [are] infinite." [63]

To the extent Cloud data impacts the court's spoliation analysis, we may well see a trend to provide a safe harbor for the party contracting for Cloud services that acted in good faith regarding issues of data management and preservation, but where the CSP failed in its duties.

3. How Is the Data Collected from the Cloud? Data Export: APIs and Other Cloud Tools

Some CSPs provide tools (some free, some paid via premium service) with which to preserve data in place ("litigation holds"), while with other CSPs, Cloud Customers may need to collect or export the data in order to preserve it. Ultimately, it is the Cloud Customer that must comply with its legal obligations, working within the confines of the CSP (and potentially its subcontractor(s)) technological processes to manage its data.

[*96]

a. Searching Cloud Data

Search tools allow search terms or other search parameters to be applied against a dataset. [64] Some of these tools can significantly reduce the scope and burden of electronic discovery. Before deciding to move information to the Cloud, an entity should discuss any analytical tools the CSP will supply, and determine whether any of the

---

[62] See N.J. Mfrs. Ins. Co. v. Hearth & Home Techs., Inc., No. 3:06- CV-2234, 2008 WL 2571227, at 7 (M.D. Pa. June 25, 2008) ("A party to a law suit, and its agents, have an affirmative responsibility to preserve relevant evidence… . A [party] … is not relieved of this responsibility merely because the [party] did not itself act in bad faith and a third party to whom [the party] entrusted the evidence was the one who discarded or lost it." (citation omitted)).

[63] *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., L.L.C., 685 F. Supp. 2d 456, 465 (S.D.N.Y 2010)*.

[64] See The Sedona Conference, The Sedona Glossary: E-Discovery & Digital Information Management (3d ed. 2010).

entity's existing tools (or tools provided by outside vendors) will work in the particular Cloud environment or whether the data has to be exported from the Cloud before those tools, usually based in forensics, can be applied. [65]

b. Collection and Production of Cloud Data

Depending on the Cloud service and the deployment model, the cost of collecting ESI from the Cloud may be significant, if not prohibitive. This cost is a factor to be considered with respect to the ESI's accessibility for e- **[*97]** discovery purposes. [66] If the cost of retrieving ESI outweighs its evidentiary value, then a producing party can claim the ESI is "not reasonably accessible because of undue burden or cost." [67]

At least one case has held that a party that moves ESI to the Cloud and thus renders it relatively less accessible compared to ESI within the enterprise, may have to bear the burden of that cost in producing the ESI. [68] Regardless, an entity should proactively address how and at what cost ESI in the Cloud can be collected for e-discovery and disclosure purposes before moving its ESI to the Cloud and failure to do so may result in significant defensibility challenges. Indeed, courts may not be persuaded by an inaccessibility/burden argument when an organization places data in the Cloud but makes no proactive provisions for recovering that data for litigation or other reasons.

Entities that regularly participate in litigation should consider:

. Whether the CSP can preserve the data in place via a technical litigation hold process, or whether the entity must collect/export the data in order to preserve;

. If the preservation of data can be accomplished via date and/or custodian;

---

[65] Forensics is the scientific examination and analysis of data held on or retrieved from ESI in such a way that the information can be used as evidence in a court of law. While forensic analysis of data is only needed in a small percentage of cases, when that information is required, it is often critical. Forensic analysis on data in the Cloud can be particularly challenging. As one commentator has noted, forensic investigation in the Cloud is more difficult, because data for multiple customers may be located on the same server, or otherwise spread across an ever-changing set of hosts and data centers. So the "cloud-based evidence may pose forensic and chain of custody problems, as accessing cloud data and ensuring it has not been contaminated may be more challenging where there may be multiple, variable storage locations for a single piece of data." Harvard Law Nat'l Sec. Research Grp., Cloud Computing and National Security Law 3 (2010).

Another practical challenge is that typically, a forensic expert must have direct access to the server or other medium upon which the information resides and, in some cases, the server must be taken offline or shut down. Similarly, "as with any live forensic examination another challenge will be the establishing of snapshots of the system in operation. But in [the case of the Cloud] one can question if this is good enough for such a "vast' and possibly globally distributed ecosystem." Jon Shende, Digital Forensic Challenges Within Cloud Computing, Sys-Con Media (Oct. 19, 2010, 11:10 AM), *http://jonshende.sys-con.com/node/1576458*. Thus, there is a big uncertainty on the capability of conducting digital forensic investigations in cloud infrastructures.

While true forensic collections on servers are not very common, when potentially relevant information is located on a Public Cloud server, it is unlikely that the entity that owns the information will have the rights or ability to physically access the servers, and even less likely that they will have the option of turning them off. In a Private Cloud, an entity may have more options available to it. Accordingly, before an entity decides to move information to the Cloud, it should clearly understand what access rights it would have under the SLA with the CSP in a case where forensic analysis is sought. Additionally, digital forensic investigators will need to adapt their techniques and practices in order to capably conduct effective investigations in cloud computing environments.

[66] It is also critical to assess the impact of Cloud data revision history and/or auto saved versions. One should request the Cloud Service Provider detail their process for allowing collection and/or segregation of this data.

[67] *Fed. R. Civ. P. 26*.

[68] See *Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal. 2007)*.

. The process by which the CSP will inform the Cloud Customer of movement of its data by the CSP to new data centers, etc.;

. How much data will typically be required for collection (i.e., Cloud Customers must understand their litigation portfolio in order to determine appropriate response times with the CSP);

. Whether data can be transmitted over a network connection or whether a local storage (and shipment of that storage) is required;

. Determine response times and format of data exports from the Cloud;

. Determine what metadata is kept in the general course of business and whether the CSP can export any and all fields if necessary without changing/altering metadata;

. Determine the impact of the preservation and collection processes on the entity's business and daily computing environment; and

[*98] . Determine controls in place that will track chain of custody.

In the traditional computing model, tools have been developed in order to provide visibility into the contents of information so that its relevance can be determined. [69]

c. How Can Cloud Data Be Used as Evidence at Trial? Rule 26(b)(2)(B) and Admissibility Information Collected from the Cloud

The rules of evidence apply to ESI and paper evidence with the same force. [70] However, there are practical differences between digital and tangible evidence that must be considered when planning trial strategy. [71]

There are several accessibility and admissibility issues that can, and should, be proactively addressed because they may reasonably be anticipated to be the subject of future discovery disputes when considering storing data in the Cloud. For instance, one of the key components of electronic discovery is being able to identify the person who created or modified a particular piece of information. [72] One common method of authenticating a document is to have the custodian who created or modified it testify as to its authenticity. But in order to do so, the custodian, or other witnesses, may be required to present evidence regarding the life cycle of the document.

This is fairly straightforward in the traditional computing model. The custodian can testify that she created and saved the document on her local computer. Other evidence can show that no other person accessed or modified it, or if they did, the potential effect on its authenticity. But this evidence may be more difficult to marshal if the document is in the Cloud. Consequently, before moving information to the Cloud, an entity should have an understanding of exactly what information the CSP creates and/or retains regarding the creation and modification of, and access to, the entity's **[*99]** information in the Cloud. Such provisions (preferably memorialized in the SLA)

---

[69] These tools include document review applications, enterprise search applications, and document repository search applications.

[70] See Manual for Complex Litigation (Fourth) § 11.447 (2004) ("In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence."); Jack B. Weinstein & Margaret Berger, *Weinstein's Federal Evidence § 901.08* (2d ed. 2007) ("No additional authenticating evidence is required" just because the records are in computerized form rather than pen or pencil and paper.).

[71] See *In re Vinhnee, 336 B.R. 437, 444-45 (B.A.P. 9th Cir. 2005)* ("The paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records.").

[72] See Kenneth N. Rashbaum, Matthew F. Knouff & Dominique Murray, Admissibility of Non-U.S. Electronic Evidence, ***18 Rich. J.L. & Tech. 1, 4 (2012)***.

should, as indicated in more detail below, assist the party who seeks to offer Cloud information to establish its authenticity.

4. Admissibility - Authentication and Other Foundation Issues

One issue related to the preservation and collection of information in the Cloud concerns doing so in a way that allows for it to be admitted as evidence. The rules of evidence apply to and must be complied with respect to ESI with the same force that they apply to more traditional types of evidence. [73] However, there are meaningful differences between digital and tangible evidence that can present important practical considerations that must be considered. [74]

In March 2008, The Sedona Conference's Commentary on ESI Evidence and Admissibility was published, and provides an in-depth overview on this particular topic. [75] As written in the Introduction of that publication:

The legal community is … grappling with whether and how ESI, once produced, can actually be authenticated and used as evidence at trial or in motion practice. As succinctly noted by Judge Grimm in a … leading case on the subject:

Considering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted. [76]

Under *Rule 104 of the Federal Rules of Evidence*, judges are charged with making preliminary rulings on admissibility of evidence. [77] Matters considered under Rule 104(a), such as the existence of a privilege or the applicability of a hearsay exception, are determined solely by the judge, who is unbound by the Federal Rules. [78] Authentication under Rule 901, however, **[*100]** is "a subset of relevancy," and is therefore considered under Rule 104(b). [79] Authentication therefore requires a "two-step process" by which the judge first considers the adequacy of the foundation for the proffered evidence, and determines whether to admit the evidence to the jury for consideration of its authenticity. [80]

Under Rule 901, authentication requires but a "minimal [foundational] showing" by its proponent: "A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be… . This is not a particularly high barrier to overcome." [81]

In the case of e-mail evidence, for instance, the Federal Rules require only that "the proponent of the evidence has "offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is.'" [82] In United States v. Safavian, which addresses the admissibility of e-mail, the District Court for the District of

---

[73] See supra note 70.

[74] See *In re Vinhnee, 336 B.R. at 444-45* ("The paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records.").

[75] The Sedona Conference Commentary on ESI Evidence & Admissibility (2008).

[76] Id. at 1 (citing *Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007)*).

[77] *Fed. R. Evid. 104*.

[78] *Lorraine, 241 F.R.D. at 539*.

[79] Id.

[80] *Id. at 538*.

[81] *Id. at 542* (citation omitted). See also *Fed. R. Evid. 901*.

Columbia explained: "The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so." [83]

Judge Grimm notes in Lorraine that while some courts have imposed "demanding requirements for authenticating" electronic records, or have otherwise "recognized a need to demonstrate the accuracy of these records," it is still the case that "more courts have tended towards the lenient rather than the demanding approach" in accepting such records as authentic. [84] At the same time, courts have recognized that, while the "pervasiveness," and thus the significance, of digital evidence has increased over time, [85] so too has the risk of tampering. [86] Some courts have suggested that the "existing framework" of the Federal Rules is adequate to address the **[*101]** admissibility of digital evidence; [87] others, however, have at least recognized that digital evidence "involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records." [88]

In authenticating a record under Rule 901(a), the Vinhnee court explained:

The focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created. [89]

This is one area where it might be more difficult to prove the authentication of ESI in the Cloud if the Provider is unable to present sufficient information regarding the life cycle of the ESI. It is critical, then, that an entity considering the Cloud perform sufficient due diligence with the CSP to understand precisely what information the Provider can present.

Conclusion

Moving information to the Cloud can provide many benefits to organizations and it can also pose significant risks. Most of these benefits and challenges can be addressed by reference to traditional principles of law, but they must

---

[82] *Lorraine, 241 F.R.D. at 542*. (emphasis added) (quoting *United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006)*).

[83] *Safavian, 435 F. Supp. 2d at 38* (emphasis in original).

[84] *Lorraine, 241 F.R.D. at 558*.

[85] *Id. at 537*.

[86] *In re Vinhnee, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005)* ("The increasing complexity of ever-developing computer technology necessitates more precise focus… . For example, digital technology makes it easier to alter text of documents that have been scanned into a database."). See also Balboa Threadworks, Inc. v. Stucky, No. 05-1157- *JTM-DWB, 2006 U.S. Dist. LEXIS 29265, at 8 (D. Kan. Mar. 24, 2006)* (noting that "electronic evidence can easily be erased and manipulated, either intentionally or unintentionally"); Graves v. Doe, No. 1:10cv44, *2010 U.S. Dist. LEXIS 41376, at 2 (D. Utah Apr. 27, 2010)* ("There is a risk that the relevant electronic evidence in possession of third parties may be altered, erased, or destroyed.").

[87] *In re F.P., 878 A.2d 91, 95 (Pa. 2005)* ("Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages… . We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of [the rules of evidence]."). See also *Lorraine, 241 F.R.D. at 538 n.5* ("Indeed, ***Fed. R. Evid. 102*** contemplates that the rules of evidence are flexible enough to accommodate future "growth and development' to address technical changes not in existence as of the codification of the rules themselves.").

[88] *In re Vinhnee, 336 B.R. at 444-45* (further noting that while, in the case of a paper record, "the foundation is … easily established," the format of digital evidence complicates inquiries into "custody, access, and procedures for assuring that the records … are not tampered with").

[89] *Id. at 444*.

be viewed through the lens of evolving technology. Jurisdiction is likely to remain a fluid concept for some time as courts adjust to the disconnect between the subject matter and its potential locations in many places at the same time. Other concepts, such as admissibility, are more amenable to resolution by reference to traditional notions of foundation, albeit with the twist that authentication and reliability may take no new significance as metadata concepts of identification of data and their paths become more familiar to lawyers and judges. At base, though, organizations should carefully weigh the benefits against the potentially **[*102]** increased difficulties of managing, preserving, collecting, reviewing, and producing information, and should consider the extent to which privacy laws and regulations must be complied with.

Cloud technology, while potentially creating a new business paradigm, will ultimately be evaluated in litigation through the bench and bar's reliance on time-tested precepts of business strategies and law. Lawyers, as they have done since the days of bound volumes of sheepskin, will still be called upon to guide businesses in giving legal and strategic advice on matters involving questions of records and information practices, balancing the benefits of cost and convenience against attenuated access and security safeguards. They will still be called upon to anticipate the hazards of the information seas and chart courses around them through an understanding of evolving technology and its challenges, preparation by assiduous negotiation of relationships and provisions for access to the information, and review and production when it is required for litigation. And lawyers will continue to be asked to advise on the protections for their clients' most sensitive communications and data which, in this era of technology advancing at cyber-speed, will rely on that most old-fashioned virtue: the hard work of due diligence as to how, and whether, the Cloud can meet some of these Information Governance challenges.